

Super-symmetric informationally complete measurements

Huangjun Zhu

*Perimeter Institute for Theoretical Physics, Waterloo, On N2L 2Y5, Canada
August 25, 2015*

Abstract

Symmetric informationally complete measurements (SICs in short) are highly symmetric structures in the Hilbert space. They possess many nice properties which render them an ideal candidate for fiducial measurements. The symmetry of SICs is intimately connected with the geometry of the quantum state space and also has profound implications for foundational studies. Here we explore those SICs that are most symmetric according to a natural criterion and show that all of them are covariant with respect to the Heisenberg-Weyl groups, which are characterized by the discrete analogy of the canonical commutation relation. Moreover, their symmetry groups are subgroups of the Clifford groups. In particular, we prove that the SIC in dimension 2, the Hesse SIC in dimension 3, and the set of Hoggar lines in dimension 8 are the only three SICs up to unitary equivalence whose symmetry groups act transitively on pairs of SIC projectors. Our work not only provides valuable insight about SICs, Heisenberg-Weyl groups, and Clifford groups, but also offers a new approach and perspective for studying many other discrete symmetric structures behind finite state quantum mechanics, such as mutually unbiased bases and discrete Wigner functions.

Keywords: Symmetric informationally complete measurements (SICs), Heisenberg-Weyl groups, Clifford groups, Super-symmetric, Hesse SIC, Hoggar lines

1. Introduction

Symmetry plays a fundamental role in all areas of natural science. Of special interest are those objects possessing highest symmetry, which are the

Email address: hzhu@pitp.ca (Huangjun Zhu)

targets of constant quest. In this paper, we are concerned with an elusive discrete symmetric structure known as *symmetric informationally complete measurements* (SICs in short) [1–5]. In a d -dimensional Hilbert space, a SIC is usually composed of d^2 subnormalized projectors onto pure states $|\psi_j\rangle\langle\psi_j|/d$ with equal pairwise fidelity,

$$|\langle\psi_j|\psi_k\rangle|^2 = \frac{d\delta_{jk} + 1}{d + 1}. \quad (1)$$

Here by a ‘‘SIC’’ we shall mean the set of SIC projectors $\Pi_j = |\psi_j\rangle\langle\psi_j|$, which sum up to d times of the identity, $\sum_j \Pi_j = dI$. SICs have many nice properties rooted in their high symmetry, which make them an ideal candidate for fiducial measurements. They play a crucial role in studying quantum Bayesianism [6] and in understanding the geometry of quantum state space [7, 8]. They are useful in linear quantum state tomography [4, 9–13], quantum cryptography [14–18], and signal processing [19]. They also have intriguing connections with many other interesting subjects, such as equiangular lines, 2-designs, mutually unbiased bases (MUB), Lie algebras, and Galois theory; see Ref. [5] and references therein.

A SIC gives rise to a regular simplex in the operator space. Although this perspective is fruitful in understanding its properties [5], it has an obvious limitation: most permutations among the SIC projectors cannot be realized by unitary or antiunitary transformations, those transformations that preserve the quantum state space. This conflict between permutation symmetry and unitary symmetry has profound implications for foundational studies and quantum information science [6–8, 20, 21]. It is closely connected to the fact that the state space is not a ball except for dimension 2. A better understanding of the symmetry of SICs is crucial to decoding the geometry of the quantum state space as well as foundational and practical issues entangled with the geometry.

How symmetric is a SIC? This is a basic question we need to answer before we can conceive a clear picture about the quantum state space. Motivated by this question, here we determine those SICs that are most symmetric according to a natural criterion. By virtue of the classification of finite simple groups (CFSG) [22, 23], we show that the SIC in dimension 2, the Hesse SIC in dimension 3 [1, 4, 24–29], and the set of Hoggar lines in dimension 8 [1, 4, 30] are the only three SICs up to unitary equivalence whose symmetry groups act transitively on pairs of SIC projectors. All these SICs are covariant with respect to Heisenberg-Weyl (HW) groups, and their symmetry groups are subgroups of Clifford groups [24, 25, 31, 32]. Moreover, only the Hesse SIC

is covariant with respect to the Clifford group. These results provide valuable insight on the elusive symmetry of SICs and geometry of the quantum state space.

Although our main focus here is the symmetry of SICs, it turns out that the approach introduced here is also surprisingly useful for studying many other discrete symmetric structures behind finite state quantum mechanics, such as HW groups, Clifford groups, MUB, discrete Wigner functions, and unitary 2-designs [21, 33]. For example, based on the present work, recently we have shown that the operator basis underlying the discrete Wigner function introduced by Wootters [34] is almost uniquely characterized by the double transitivity of its symmetry group [21], which turns out to be equivalent to its symmetry group being a unitary 2-design [35]. These conclusions establish the unique status of the Wootters discrete Wigner function over all other quasi-probability representations of quantum mechanics. The ramifications of the present work are still under exploration.

The rest of the paper is organized as follows. In Sec. 2 we introduce the background and the concept of super-symmetric informationally complete measurements (super-SICs for short). In Sec. 3 we state our main results. In Sec. 4 we establish the equivalence of several symmetry properties of SICs. In Sec. 5 we derive a necessary condition for the existence of super-SICs based on triple products among SIC projectors. In Sec. 6 we determine all super-SICs in prime power dimensions. In Sec. 7 we reveal a remarkable connection between super-SICs and the HW group, thereby determining all super-SICs. Section 8 summarizes this paper. Some technical details are relegated to the appendix.

2. Setting the stage

2.1. Symmetry of SICs

The *symmetry group* \overline{G} of a SIC $\{\Pi_j\}$ is composed of all unitary operators U that leave the set of SIC projectors invariant; that is, $U\Pi_jU^\dagger = \Pi_{\sigma(j)}$ for a suitable permutation σ . By convention, operators that differ only by overall phase factors are identified, as indicated by the overline notation in “ \overline{G} ”. The *extended symmetry group* is the larger group that contains also antiunitary operators. Every SIC known so far is *group covariant* in the sense that it can be generated from a single state—the *fiducial state*—by a group composed of unitary operators, that is, the SIC projectors form a single orbit under the action of the symmetry group. In addition, every known SIC is covariant with respect to one or another version of the HW group [4], and this is true for every SIC in dimension 3 [36]. In particular, every known SIC is sharply

covariant in the sense that the generating group can be chosen to have the minimal possible order, that is, the number of SIC projectors. By contrast, sharply covariant MUB are quite rare; actually, only two examples are known [37, 38].

How much additional symmetry can we expect beyond group covariance? To understand the significance of this question, it is instructive to compare a SIC in dimension d with the regular simplex in the operator space defined by the SIC [5]. The isometry group of the regular simplex is isomorphic to the full permutation group of d^2 letters, which can realize any permutation among the vertices. However, most of these permutations cannot be realized by unitary or antiunitary transformations, those transformations that leave the quantum state space invariant, because the state space is not a ball except in dimension 2. A natural question to ask is to what extent the permutation symmetry can be retained given this limitation. Such surviving symmetry is closely related to the geometry of the quantum state space, so any progress concerning this subject may potentially lead to a clearer picture about the quantum state space.

To answer the question posed above, we need to introduce several new concepts. A SIC is *k-covariant* if every ordered k -tuple of SIC projectors can be mapped to every other such k -tuple within its symmetry group; that is, its symmetry group acts k -transitively in the language of permutation groups [39, 40]; see Appendix C for a short introduction. A k -covariant SIC is also referred to as doubly covariant when $k = 2$ and triply covariant when $k = 3$. As we shall see shortly, no triply covariant SICs can exist. For this reason doubly covariant SICs are called *super-symmetric* since they represent the most symmetric structure that can appear in the Hilbert space.

To complete the picture, a SIC is *k-homogeneous* if every unordered k -tuple of SIC projectors can be mapped to every other such k -tuple under its symmetry group. A SIC in dimension d is k -homogeneous if and only if it is $(d^2 - k)$ -homogeneous. In addition, any k -covariant SIC is k -homogeneous (the converse is also true when $k \leq d^2/2$ according to Lemma 2 in Sec. 4, but is not so obvious). When the symmetry group is replaced by the extended symmetry group, the terminologies are modified by adding the prefix “quasi”. For example, a SIC is quasi-super-symmetric if every two ordered pairs of SIC projectors can be mapped to each other under its extended symmetry group.

The concepts introduced above also apply to operator bases and generalized measurements [21]. In this paper, however, we shall focus on SICs.

2.2. Heisenberg-Weyl groups and Clifford groups

To make this paper self-contained, here we present a short introduction about HW groups and Clifford groups; see Refs. [4, 24, 25, 31, 32, 41] for more details.

The HW group is generated by the phase operator Z and the cyclic shift operator X defined by their action on the kets $|e_r\rangle$ of the “computational basis”,

$$Z|e_r\rangle = \omega^r|e_r\rangle, \quad X|e_r\rangle = |e_{r+1}\rangle, \quad (2)$$

where $\omega = e^{2\pi i/d}$, $r \in \mathbb{Z}_d$, and \mathbb{Z}_d is the ring of integers modulo d . The two generators obey the canonical commutation relation

$$XZX^{-1}Z^{-1} = \omega^{-1}, \quad (3)$$

which determines the HW group up to unitary equivalence and overall phase factors [42].

In this paper, it turns out that another version of the HW group, called the multipartite HW group, is more relevant to our study. This HW group D is defined only in prime power dimensions. It coincides with the HW group defined above in every prime dimension p . In prime power dimension $q = p^n$, the multipartite HW group is the tensor power of n copies of the HW group in dimension p . The elements in the multipartite HW are called displacement operators (or Weyl operators). Up to phase factors, they can be labeled by vectors of length $2n$ defined over $\mathbb{F}_p = \mathbb{Z}_p$ as

$$D_\mu = \tau^{\sum_j \mu_j \mu_{n+j}} \prod_{j=1}^n X_j^{\mu_j} Z_j^{\mu_{n+j}}, \quad (4)$$

where $\tau = -e^{\pi i/p}$, while Z_j and X_j are the phase operator and cyclic shift operator of the j th party, as defined in Eq. (2) with $d = p$. These operators satisfy the commutation relation

$$D_\mu D_\nu D_\mu^\dagger D_\nu^\dagger = \omega^{\langle \mu, \nu \rangle}, \quad (5)$$

where $\langle \mu, \nu \rangle = \mu^T J \nu$ is the symplectic product with $J = \begin{pmatrix} 0_n & -1_n \\ 1_n & 0_n \end{pmatrix}$. Two displacement operators D_μ and D_ν commute if and only if the corresponding symplectic product $\langle \mu, \nu \rangle$ vanishes. The vectors μ together with the symplectic product form a symplectic space \mathbb{F}_p^{2n} of dimension $2n$. The group of linear transformations that preserve the symplectic product is known as the

symplectic group and denoted by $\text{Sp}(2n, p)$ [43], which has order

$$p^{n^2} \prod_{j=1}^n (p^{2j} - 1). \quad (6)$$

The multipartite HW group defines a faithful irreducible projective representation of an elementary abelian group, recall that a group is elementary abelian if it is abelian and all elements other than the identity have the same order, which is a prime. The converse is shown in the following lemma.

Lemma 1. *Suppose H is an elementary abelian group of order p^{2n} with p a prime and n a positive integer. Then every faithful irreducible projective representation of H has degree p^n and the image is (projectively) unitarily equivalent to the multipartite HW group in dimension p^n .*

Remark 1. Although this lemma is known as folklore, it is difficult to find an explicit statement in the literature; see Refs. [31, 32, 44] for relevant conclusions. A self-contained proof is presented in the appendix.

The Clifford group C is the normalizer of the multipartite HW group, that is, the group composed of all unitary operators that leave the multipartite HW group invariant up to phase factors [4, 24, 31, 32, 41]. Any Clifford unitary U induces a linear transformation on the symplectic space that labels the displacement operators. This linear transformation necessarily belongs to the symplectic group $\text{Sp}(2n, p)$ since conjugation preserves the commutation relation, so the induced linear transformation preserves the symplectic product. Conversely, given any symplectic matrix F , there exist q^2 Clifford unitaries (up to phase factors) that induce F , which differ from each other by displacement operators [31, 32]. The quotient group $\overline{C}/\overline{D}$ (\overline{G} denotes the group G modulo phase factors) can be identified with the symplectic group $\text{Sp}(2n, p)$. The Clifford group \overline{C} in dimension p^n has order

$$p^{n^2+2n} \prod_{j=1}^n (p^{2j} - 1). \quad (7)$$

Note that the symplectic group $\text{Sp}(2, p)$ in the special case $n = 1$ can be identified with the special linear group $\text{SL}(2, p)$. When p is odd, \overline{C} is isomorphic to the affine symplectic group $\text{ASp}(2n, p) = \text{Sp}(2n, p) \ltimes \mathbb{F}_p^{2n}$ [31, 32].

3. Main results

After careful inspection of all SICs known in the literature [4], we find three super-SICs (SICs that are super-symmetric). The first obvious candidate is the SIC in dimension 2, whose symmetry group can realize all even permutations among the SIC projectors (this SIC is also quasi-4-covariant, since the extended symmetry group can realize all permutations).

The second super-SIC is the *Hesse SIC* in dimension 3 [1, 4, 24–29], which is generated by the HW group from the fiducial ket

$$\frac{1}{\sqrt{2}}(0, 1, -1)^T. \quad (8)$$

It is the only known SIC whose symmetry group is the whole Clifford group, which has order 9×24 in dimension 3 [25]. The Hesse SIC also has an intimate connection with the discrete Wigner function introduced by Wootters [34]. Let Π_j be SIC projectors in the Hesse SIC, then $1 - 2\Pi_j$ happen to be phase point operators underlying the Wootters discrete Wigner function. This result is not a mere coincidence, but has deep reasons, as explained in Ref. [21].

The third super-SIC is the set of *Hoggar lines* [1, 4, 30] generated by the three-qubit Pauli group (the multipartite HW group in dimension 8) from

$$\frac{1}{\sqrt{6}}(1 + i, 0, -1, 1, -i, -1, 0, 0)^T. \quad (9)$$

It has an exceptionally large symmetry group, which has order 64×6048 [4]¹. It is the only SIC known so far that is not covariant with respect to the usual HW group defined in Eq. (2) and also the only known SIC that is covariant with respect to the multipartite HW group in a dimension that is not prime [4]. In addition, since all SIC projectors are connected by local unitary transformations, they all have the same entanglement. Such SICs are interesting but quite rare in prime power dimensions, although there is another example in dimension 4 [4, 45, 46].

It turns out that the three super-SICs we have identified exhaust all possibilities.

¹The stabilizer of each fiducial state in the set of Hoggar lines is a nonabelian simple group of order 6048, which turns out to be isomorphic to the projective special unitary group PSU(3, 3).

Theorem 1 (CFSG). *The SIC in dimension 2, the Hesse SIC in dimension 3, and the set of Hoggar lines in dimension 8 are the only three (quasi)-super-SICs up to unitary equivalence. They are also the only three (quasi)-2-homogeneous SICs up to unitary equivalence.*

Remark 2. The full proof of Theorem 1 relies on the classification of 2-transitive permutation groups [39, 40, 47–49], which in turn relies on the CFSG [22, 23]. To make room for future improvement, we mark all theorems and lemmas with “CFSG” whenever CFSG is involved in the proofs. In the case of prime power dimensions, nevertheless, we can prove Theorem 1 without the CFSG; see Theorem 2 in Sec. 6. In addition, we try to prove as much as possible without resorting to such heavy tools; the CFSG is required directly only in the proof of Lemma 13 in Sec. 7.

In sharp contrast with SICs, all the operator bases underlying the Wootters discrete Wigner functions [34] are super-symmetric [21]. Theorem 1 shows that the restriction to pure states imposes a stringent limitation on the potential symmetry of an operator basis. This observation is instructive to understanding quasi-probability representations of quantum mechanics and may have implications for foundations studies, such as quantum Bayesianism [6, 20].

4. Equivalence of 2-homogeneous SICs and super-SICs

Although the requirement of k -covariance is a priori much stronger than that of k -homogeneity whenever $k > 1$, it turns out that the two requirements are equivalent for SICs as long as $k \leq d^2/2$.

Lemma 2. *A SIC in dimension d is (quasi)- k -covariant with $k \leq d^2/2$ if and only if it is (quasi)- k -homogeneous. In particular, a SIC is (quasi)-super-symmetric if and only if it is (quasi)-2-homogeneous.*

Proof. The claims are obvious when $k = 1$. When $k \geq 2$, according to Theorem 1 of Kantor [50] and Theorem 9.4B in Ref. [39], any k -homogeneous permutation group of degree $n \geq 2k$ is $(k-1)$ -transitive. If n is a perfect square, then the group is also k -transitive, except possibly some 4-homogeneous permutation group G of degree 9. In addition, such a group G must contain a subgroup isomorphic to $\text{PSL}(2, 8)$, which is a nonabelian simple group. These facts confirm the lemma immediately except when the dimension is equal to 3 and the SIC is (quasi)-4-homogeneous. In this special case, the SIC is (quasi)-triply covariant and is thus group covariant. Any group covariant SIC in dimension 3 is covariant with respect to the HW group, and its

extended symmetry group is a subgroup of the extended Clifford group [25]; actually, this is true for any SIC in dimension 3 according to Ref. [36]. However, the extended Clifford group in dimension 3 is solvable and thus cannot contain any subgroup isomorphic to $\text{PSL}(2, 8)$. Alternatively, this special case can be excluded by Lemma 6 in Sec. 5. \square

In view of Lemma 2, the second part of Theorem 1 is an immediate consequence of the first part. Therefore, we can focus on (quasi)-super-SICs in the rest of the paper.

When the dimension is even, we have another equivalence relation.

Lemma 3. *Every quasi-super-SIC in an even dimension is a super-SIC.*

Remark 3. Although this lemma also holds when the dimension is odd, so far we can prove this conclusion only after the classification of all quasi-super-SICs.

Lemma 3 is an immediate consequence of the following lemma, note that the symmetry group of a SIC is a subgroup of the extended symmetry group of index at most 2.

Lemma 4. *Any index-2 subgroup of a 2-transitive permutation group of even degree at least 4 is 2-transitive.*

Proof. Suppose H is an index-2 subgroup of the 2-transitive permutation group G on Ω with $|\Omega| \geq 4$. Then H is normal in G and acts transitively on Ω . Let $S \in G$ be the stabilizer of a given point in Ω , say α , then S acts transitively on $\Omega \setminus \alpha$. Let $R = S \cap H$; then R is an index-2 normal subgroup of S . Therefore, R is either transitive on $\Omega \setminus \alpha$ or has two orbits of equal length. When the degree $|\Omega|$ is even, however, the latter scenario cannot happen since the cardinality of $\Omega \setminus \alpha$ is odd. So R is transitive on $\Omega \setminus \alpha$, and H is 2-transitive on Ω . \square

5. Symmetry and triple products

Before proving our main result, we first show that no triply covariant SICs can exist and that for prime-power dimensions, (quasi)-super-SICs can only exist in dimensions 2, 3, and 8. The proofs are based on simple observation on triple products among SIC projectors,

$$T_{jkl} = \text{tr}(\Pi_j \Pi_k \Pi_l). \quad (10)$$

Such triple products have played an important role in studying the symmetry of and equivalence relations among SICs [4, 25, 51]. They are also useful to studying discrete Wigner functions [34]. Note that $|T_{jkl}|$ is equal to $(d+1)^{-3/2}$ if the three indices are distinct, while it is equal to $1/(d+1)$ or 1 if two or three indices coincide. The normalized triple products $\tilde{T}_{jkl} = T_{jkl}/|T_{jkl}|$ satisfy

$$\tilde{T}_{jkl} = \tilde{T}_{klj} = \tilde{T}_{ljk} = \tilde{T}_{jlk}^* = \tilde{T}_{ljk}^* = \tilde{T}_{kjl}^*, \quad (11)$$

$$\tilde{T}_{jkl} = \tilde{T}_{mjk} \tilde{T}_{mkl} \tilde{T}_{mlj}. \quad (12)$$

Lemma 5. *No SIC is triply covariant.*

Remark 4. If a SIC is triply covariant, then all triple products among distinct SIC projectors are equal. Consequently, all permutations among SIC projectors can be realized by unitary transformations according to Theorem 3 in Ref. [51] (see also Chap. 10 in Ref. [4]). Such a SIC would be too symmetric to exist!

Proof. Suppose on the contrary that the SIC $\{\Pi_j\}$ is triply covariant. Then each \tilde{T}_{jkl} for distinct j, k, l equals ± 1 , where the sign is independent of j, k, l , so

$$\sum_l T_{jkl} = \pm \frac{d^2 - 2}{(d+1)^{3/2}} + \frac{2}{d+1}, \quad j \neq k. \quad (13)$$

Since the SIC projectors Π_l sum up to d times of the identity, we also have

$$\sum_l T_{jkl} = d \operatorname{tr}(\Pi_j \Pi_k) = \frac{d}{d+1}. \quad (14)$$

However, the two equations above cannot be satisfied simultaneously. This contradiction completes the proof. \square

Lemma 6. *No SIC in dimension $d \geq 3$ is quasi-triply covariant.*

Since this lemma is not essential in proving our main result, the proof is relegated to the appendix.

Lemma 7. *Suppose there exists a quasi-super-SIC in prime-power dimension d . Then d equals 2, 3, or 8.*

This lemma follows from Lemmas 8, 9, and 10 below.

Lemma 8. *Suppose $\{\Pi_j\}$ is a quasi-super-SIC with normalized triple products \tilde{T}_{jkl} . Then all \tilde{T}_{jkl} are $2d^2$ th roots of unity, that is, $\tilde{T}_{jkl}^{2d^2} = 1$.*

Proof. If $\{\Pi_j\}$ is super-symmetric, then the multiset $\{\tilde{T}_{mjk}\}_{m=1}^{d^2}$ is identical with $\{\tilde{T}_{mkj}\}_{m=1}^{d^2}$. On the other hand, the two multisets are conjugates of each other. Therefore, both of them are conjugation invariant and $\prod_m \tilde{T}_{mjk} = \pm 1$, where the sign is independent of j and k as long as they are distinct. Now taking the product over m in Eq. (12) yields $\tilde{T}_{jkl}^{d^2} = \pm 1$, which implies the lemma.

If $\{\Pi_j\}$ is quasi-super-symmetric but not super-symmetric, then $\{\Pi_j\}$ is quasi-2-homogenous but not 2-homogenous according to Lemma 2. It follows that every ordered pair of distinct SIC projectors can be mapped to the same pair with the reverse order under the symmetry group. So the multiset $\{\tilde{T}_{mjk}\}_{m=1}^{d^2}$ is still conjugation invariant and the lemma holds as before. \square

Lemma 9. *Suppose there exists a quasi-super-SIC in dimension $d \geq 3$, then $(d-2)\sqrt{d+1} \in \mathbb{Z}[\zeta_{2d^2}]$ and $\sqrt{d+1} \in \mathbb{Q}[\zeta_{2d^2}]$, where ζ_{2d^2} is a primitive $2d^2$ th root of unity.*

Remark 5. Here $\mathbb{Z}[\zeta_{2d^2}]$ is the extension of the ring of integers by ζ_{2d^2} , and $\mathbb{Q}[\zeta_{2d^2}]$ is the extension of the field of rational numbers by ζ_{2d^2} [52].

Proof. From the two equations

$$\begin{aligned} \sum_k \text{tr}(\Pi_j \Pi_k \Pi_l) &= \frac{2}{d+1} + \sum_{k \neq j, l} \frac{1}{(d+1)^{3/2}} \tilde{T}_{jkl}, \\ \sum_k \text{tr}(\Pi_j \Pi_k \Pi_l) &= d \text{tr}(\Pi_j \Pi_l) = \frac{d}{d+1}, \quad j \neq l, \end{aligned} \tag{15}$$

we deduce that

$$\sum_{k \neq j, l} \tilde{T}_{jkl} = (d-2)\sqrt{d+1}. \tag{16}$$

The lemma follows from the fact that \tilde{T}_{jkl} are $2d^2$ th roots of unity according to Lemma 8. \square

Now Lemma 7 is a consequence of Lemma 9 and the following lemma.

Lemma 10. *Suppose d is a prime power. Then $\sqrt{d+1} \in \mathbb{Q}[\zeta_{2d^2}]$ if and only if $d = 3, 8$.*

Proof. Suppose $\sqrt{d+1} \in \mathbb{Q}[\zeta_{2d^2}]$. Then $\sqrt{d+1}$ belongs to \mathbb{Q} or a quadratic extension of \mathbb{Q} . In the former case $d+1$ must be a perfect square, which

implies that $d = 3, 8$ given that d is a prime power (cf. Lemma 15 in the appendix).

Observing that $\mathbb{Q}[\zeta_{2d^2}]$ is a Galois extension of \mathbb{Q} , we conclude that the quadratic extensions of \mathbb{Q} contained in $\mathbb{Q}[\zeta_{2d^2}]$ are in one-to-one correspondence with the subgroups of the Galois group $\text{Gal}(\mathbb{Q}[\zeta_{2d^2}]/\mathbb{Q})$ of index 2 [52]. The group $\text{Gal}(\mathbb{Q}[\zeta_{2d^2}]/\mathbb{Q})$ is isomorphic to the automorphism group of \mathbb{Z}_{2d^2} , which in turn is isomorphic to the multiplicative group $\mathbb{Z}_{2d^2}^*$ of invertible elements (or units) in \mathbb{Z}_{2d^2} [53].

When d is a power of 2, $\mathbb{Z}_{2d^2}^*$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{d^2/2}$, which contains three subgroups of index 2. Consequently, $\mathbb{Q}[\zeta_{2d^2}]$ contains three quadratic extensions over \mathbb{Q} , which are identical with the three quadratic extensions over \mathbb{Q} contained in $\mathbb{Q}[\zeta_8]$. It is easy to verify that the three quadratic extensions are $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[i]$, and $\mathbb{Q}[\sqrt{2}i]$, none of which can contain $\sqrt{d+1}$ except when $d = 8$.

When $d = p^n$ is a power of an odd prime p , $\mathbb{Z}_{2d^2}^*$ is cyclic of order $p^{2n-1}(p-1)$ and contains a unique subgroup of index 2. Consequently, $\mathbb{Q}[\zeta_{2d^2}]$ contains a unique quadratic extension over \mathbb{Q} , which is identical with the quadratic extension over \mathbb{Q} contained in $\mathbb{Q}[\zeta_p]$. According to the famous quadratic reciprocity (see Proposition 7-3-1 in Ref. [54] for example), this unique quadratic extension is $\mathbb{Q}[\sqrt{(-1)^{(p-1)/2}p}]$, which cannot contain $\sqrt{d+1}$ except when $d = p = 3$. \square

6. Super-SICs in prime power dimensions

In this section we prove Theorem 1 in the case of prime power dimensions without resorting to the CFSG.

Theorem 2. *In prime power dimensions, the SIC in dimension 2, the Hesse SIC in dimension 3, and the set of Hoggar lines in dimension 8 are the only three (quasi)-super-SICs up to unitary equivalence. They are also the only three (quasi)-2-homogeneous SICs up to unitary equivalence.*

To achieve our goal, we need to introduce several basic results concerning permutation groups [39, 40]; see Appendix C for a short introduction on this subject.

Theorem 3 (Burnside). *Any 2-transitive permutation group G on a finite set Ω has a unique minimal normal subgroup, which is either elementary abelian acting regularly on or nonabelian simple acting primitively on Ω .*

Remark 6. A minimal normal subgroup N of a group G is a normal subgroup other than the identity that contains no other nontrivial normal subgroup of

G . A group action is *regular* if it is transitive with trivial point stabilizer; it is *primitive* if it is transitive and preserves no nontrivial partition. If N is regular elementary abelian, then it can be identified as a vector space over some finite Galois field, and G as a subgroup of the group of affine semilinear transformations on the vector space and is called *affine*. If N is nonabelian simple, then G can be identified as a subgroup of the automorphism group of N and is called *almost simple* [39, 40].

Another useful tool in our study is the following lemma reproduced from Lemma 7.2 and Theorem 7.3 in the author's thesis [4] (see also Ref. [37] and Theorem 2.34 in Ref. [1]).

Lemma 11. *Suppose \overline{G} is a subgroup of the symmetry group of a SIC. Then the number of orbits of \overline{G} on the SIC is equal to the sum of squared multiplicities of all the inequivalent irreducible components of \overline{G} . In particular, \overline{G} acts transitively on the SIC if and only if it is irreducible.*

Proof of Theorem 2. In view of Lemmas 2 and 7, to prove Theorem 2, it remains to show the uniqueness of quasi-super-SICs in dimensions 2, 3 and 8. Note that every quasi-super-SIC is necessarily group covariant.

In dimension 2, every SIC defines a regular tetrahedron on the Bloch sphere, so all SICs are unitarily equivalent.

In dimension 3, every (group covariant) SIC is covariant with respect to the HW group and its symmetry group is a subgroup of the Clifford group, which is isomorphic to $\text{SL}(2, 3) \ltimes (\mathbb{Z}_3)^2$ [4, 25, 36]. Therefore, the stabilizer of each SIC projector is isomorphic to a subgroup of $\text{SL}(2, 3)$. If the SIC is quasi-super-symmetric, then the order of the stabilizer (within the symmetry group) is divisible by 4. Observing that $\text{SL}(2, 3)$ contains a unique element of order 2, we conclude that the stabilizer contains an element of order 4. Since all order-4 Clifford unitary transformations in dimension 3 are conjugate to each other [25], without loss of generality we may assume that one fiducial ket is stabilized by (is an eigenket of) the order-4 Clifford unitary transformation

$$\frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \quad (17)$$

which happens to be the Fourier matrix in dimension 3. Calculation shows that this unitary transformation has three nondegenerate eigenkets, one of which happens to be the fiducial ket that generates the Hesse SIC (see Eq. (8)), while the other two are not fiducial kets. Therefore, the Hesse SIC is the only quasi-super-SIC in dimension 3 up to unitary equivalence.

It remains to consider quasi-super-SICs in dimension 8. Suppose $\{\Pi_j\}$ is a quasi-super-SIC in dimension 8. According to Lemma 3, $\{\Pi_j\}$ is super-symmetric, so its symmetry group \overline{G} is a 2-transitive (and automatically primitive) permutation group of degree 64. According to Theorem 3, \overline{G} is either affine or almost simple and has a unique minimal normal subgroup, say \overline{N} , which is either regular elementary abelian or nonabelian simple. According to Appendix B in Ref. [39], all 2-transitive permutation groups of degree 64 are of affine type except for the symmetric group and alternating group, which are 64 and 62 fold transitive, respectively. In view of Lemma 5, \overline{G} can be isomorphic to neither the symmetric group nor the alternating group of degree 64. Therefore, \overline{G} is an affine 2-transitive permutation group, and \overline{N} is regular elementary abelian. The group \overline{N} is necessarily irreducible according to Lemma 11 and thus defines a faithful irreducible projective representation of an elementary abelian group. According to Lemma 1, \overline{N} is unitarily equivalent to the multipartite HW group in dimension 8, that is, the three-qubit Pauli group. Consequently, \overline{G} is a subgroup of the Clifford group, which has order $2^{15} \cdot 3^4 \cdot 5 \cdot 7$ according to Eq. (7).

Suppose $|\psi\rangle$ is a fiducial ket of the three-qubit Pauli group that generates a quasi-super-SIC. Then its stabilizer contains an order-7 Clifford unitary transformation. Observe that all Sylow 7-subgroups of the Clifford group are cyclic of order 7 and are conjugate to each other. Without loss of generality, we may assume that $|\psi\rangle$ is stabilized by the order-7 Clifford unitary transformation [4]

$$U_7 \triangleq \frac{\omega^5}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 1 & 0 & -i & 0 & 0 & 0 \\ 0 & 0 & i & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -i & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & -i & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -i & 0 \\ -i & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -i & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & i \end{pmatrix}, \quad (18)$$

where $\omega = e^{2\pi i/8}$. Calculation shows that U_7 has six nondegenerate eigenkets, none of which are fiducial kets. The two-dimensional eigenspace corresponding to the eigenvalue 1 contains two fiducial kets, which happen to be the only two normalized kets in the eigenspace that satisfy the following three

equations,

$$\langle \psi | \sigma_z \otimes 1 \otimes 1 | \psi \rangle = \pm \frac{1}{3}, \quad \langle \psi | 1 \otimes \sigma_z \otimes 1 | \psi \rangle = \pm \frac{1}{3}, \quad \langle \psi | 1 \otimes \sigma_x \otimes 1 | \psi \rangle = \pm \frac{1}{3}. \quad (19)$$

The first fiducial ket happens to be the one that generates the set of Hoggar lines (see Eq. (9)). The second one

$$\frac{1}{\sqrt{6}}(-i, -1, 0, 0, -1 + i, 0, 1, 1)^T \quad (20)$$

generates a SIC which turns out to be equivalent to the set of Hoggar lines under the Clifford unitary transformation

$$\begin{pmatrix} 0 & U \\ V & 0 \end{pmatrix}, \quad U = \text{diag}(-i, -i, -1, 1), \quad V = \text{diag}(1, 1, i, -i). \quad (21)$$

This transformation was computed using the algorithm described in Chap. 10 of the author's thesis [25]. Therefore, the set of Hoggar lines is the unique quasi-super-SIC in dimension 8 up to unitary equivalence. \square

7. Super-SICs and the Heisenberg-Weyl group

In this section we prove our main result Theorem 1. In view of Theorem 2, it suffices to show that super-SICs can only exist in prime power dimensions. Here we not only prove this conclusion but also establish a remarkable connection between super-SICs and the multipartite HW group, which is of independent interest.

Theorem 4 (CFSG). *Every quasi-super-SIC is covariant with respect to the multipartite HW group in a prime power dimension; its (extended) symmetry group is a subgroup of the (extended) Clifford group.*

Remark 7. Surprisingly, the symmetry requirement on a SIC naturally leads to the canonical commutation relation and the multipartite HW group. When the dimension is a prime, this conclusion is consistent with the earlier conclusion of the author [25] that every group covariant SIC is covariant with respect to the HW group and that its (extended) symmetry group is a subgroup of the (extended) Clifford group. Recently, we have generalized Theorem 4 to operator bases, which plays a crucial role in understanding the discrete Wigner function [21]. In addition, Theorem 4 is useful to studying unitary 2-designs [35].

To prove Theorem 4, we need two additional technical lemmas, whose proofs are relegated to the appendix.

Lemma 12. *Suppose H is a subgroup of index 2 of a 2-transitive permutation group G with $|G| > 2$ on Ω . Then H has a unique minimal normal subgroup, which coincides with the unique minimal normal subgroup of G .*

Lemma 13 (CFSG). *Suppose G is an almost simple 2-transitive permutation group whose degree n is a perfect square. Let N be the minimal normal subgroup of G . Then one of the following three cases holds.*

1. N is isomorphic to the alternating group A_n with $n \geq 5$ a perfect square.
2. N is isomorphic to $\text{PSL}(k, q)$ with $(k, q) = (2, 8), (4, 7)$, or $(5, 3)$, and n is equal to 3^2 , 20^2 , or 11^2 accordingly.
3. N is isomorphic to $\text{Sp}(6, 2)$, and n is equal to 6^2 .

Remark 8. Here the symbols n, q are independent of those appearing in Sec. 2.2. The proof of this lemma relies on the classification of almost simple 2-transitive permutation groups [39, 40], which in turn relies on the CFSG [22, 23]. All other results in this paper that rely on the CFSG rely on this lemma either directly or indirectly.

Lemma 14 (CFSG). *The symmetry group and extended symmetry group of any quasi-super-SIC have a unique and identical minimal normal subgroup, which is elementary abelian and regular.*

Proof. Let $\{\Pi_j\}$ be a quasi-super-SIC with symmetry group \overline{G} and extended symmetry group \overline{EG} . Then \overline{G} is either identical with \overline{EG} or is a subgroup of index 2. So \overline{G} and \overline{EG} have a unique and common minimal normal subgroup according to Theorem 3 and Lemma 12. In addition, the minimal normal subgroup \overline{N} acts transitively on the set of SIC projectors and is thus irreducible according to Lemma 11.

Suppose on the contrary that \overline{N} is not elementary abelian or regular. Then \overline{N} is a nonabelian simple group, and \overline{EG} is an almost simple 2-transitive permutation group of degree d^2 , which is a perfect square. According to Lemma 5, \overline{N} cannot be isomorphic to A_n for $n \geq 5$, because A_n is $(n-2)$ -transitive [39, 40]. In view of Lemma 13, \overline{N} is a faithful irreducible projective representation (over the complex numbers) of $\text{PSL}(k, q)$ with $(k, q) = (2, 8), (4, 7), (5, 3)$, or $\text{Sp}(6, 2)$, and the degree of the representation (which equals the square root of the degree of the permutation group) is 3, 20, 11, or 6, respectively. According to Table II in Ref. [55], however,

the minimal degree of such a representation is 7, 399, 120, or 7. The same reasoning can also be used to exclude the alternating group A_n (without relying on Lemma 5) given that the minimal degree of such a representation for A_n is $n - 1$ when $n \geq 8$ [56]. This contradiction completes the proof. \square

Proof of Theorem 4. Suppose $\{\Pi_j\}$ is a quasi-super-SIC in dimension d with symmetry group \overline{G} and extended symmetry group \overline{EG} . Then \overline{G} and \overline{EG} have a unique common minimal normal subgroup, say \overline{N} . In addition, \overline{N} is elementary abelian and acts regularly on the set of SIC projectors according to Lemma 14. Therefore, \overline{N} has order d^2 and is irreducible according to Lemma 11. In a word, \overline{N} is a faithful irreducible projective representation of an elementary abelian group, so it is (projectively) unitarily equivalent to the multipartite HW group according to Lemma 1. Given that \overline{N} is normal in \overline{G} and \overline{EG} , we conclude that \overline{G} (\overline{EG}) is a subgroup of the Clifford group (extended Clifford group). \square

Finally, we can determine all super-SICs, thereby achieving our main goal.

Proof of Theorem 1. Theorem 1 is an immediate consequence of Theorems 2 and 4. \square

8. Summary

We have introduced super-SICs as the most symmetric structure that can appear in the Hilbert space. We proved that the SIC in dimension 2, the Hesse SIC in dimension 3, and the set of Hoggar lines in dimension 8 are the only three super-SICs up to unitary equivalence. Such general statements are of intrinsic interest but are quite rare in the literature due to the enormous difficulty in decoding elusive SICs. Our work provides valuable insight on symmetry of SICs and geometry of the quantum state space, which may have implications for foundational studies, such as quantum Bayesianism. Our work also reveals an intriguing connection between symmetry and the canonical commutation relation, which deserves further study. In addition, the ideas and techniques introduced here are quite helpful to studying MUB, discrete Wigner functions, and unitary 2-designs etc. Furthermore, our work establishes diverse links between SICs and various other subjects, such as number theory, representation theory, combinatorics, and theory of permutation groups, which are of interest to researchers from respective fields.

Acknowledgements

The author is grateful to Dragomir Ž Đoković for simplifying the proof of Lemma 12, to Gergely Harcos for helping proving Lemma 18 in the appendix, and to Daniel El-Baz for recommending Ref. [57]. The author also thanks Marcus Appleby, Ingemar Bengtsson, Lin Chen, Markus Grassl, and Mark Howard for discussions and suggestions. This work is supported in part by Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation.

Appendix A. Proof of Lemma 1

Proof. This lemma is closely related to Weyl's theorem that the HW group is uniquely characterized by the discrete analogy of the canonical commutation relation [42]. Suppose H has a d -dimensional faithful irreducible projective representation $A \mapsto U_A$ for $A \in H$. Let A_1 be an arbitrary element in H other than the identity. Given that the representation is faithful, U_{A_1} cannot be proportional to the identity and thus cannot commute with all elements in the representation according to Schur's lemma. So there exists an element $B_1 \in H$ such that

$$U_{A_1} U_{B_1} U_{A_1}^\dagger U_{B_1}^\dagger = e^{i\phi} \quad (\text{A.1})$$

with $e^{i\phi} \neq 1$ a phase factor. Observing that $U_{B_1}^p$ is proportional to the identity, we conclude that $e^{i\phi}$ is a p th root of unity. Replacing B_1 with a suitable power if necessary, we may assume that

$$U_{A_1} U_{B_1} U_{A_1}^\dagger U_{B_1}^\dagger = \omega^{-1}, \quad (\text{A.2})$$

where $\omega = e^{2\pi i/p}$ is a primitive p th root of unity. Note that A_1 and B_1 generate a group H_1 of order p^2 . If $n = 1$, then $H = H_1$, the representation must have degree p , and the image is (projectively) unitarily equivalent to the HW group in dimension p according to Weyl's theorem [25].

If $n > 1$, let A_2 be an arbitrary element in H not contained in H_1 . Then U_{A_2} commutes with U_{A_1} and U_{B_1} up to phase factors that are p th roots of unity. By multiplying A_2 with a suitable element in H_1 if necessary, we can ensure that U_{A_2} commutes with U_{A_1}, U_{B_1} and, consequently, the representations of all elements in H_1 . By the same reasoning as in the previous paragraph, there exists an element $B_2 \in H$ such that

$$U_{A_2} U_{B_2} U_{A_2}^\dagger U_{B_2}^\dagger = \omega^{-1}. \quad (\text{A.3})$$

Note that B_2 cannot belong to H_1 . By multiplying B_2 with a suitable element in H_1 if necessary, we may assume that U_{B_2} commutes with U_{A_1} and U_{B_1} . Continuing this procedure, we can eventually find n pairs of generators $A_1, B_1, \dots, A_n, B_n$ of H such that $U_{A_1}, U_{B_1}, \dots, U_{A_n}, U_{B_n}$ satisfy the canonical commutation relations

$$\begin{aligned} U_{A_j} U_{B_k} U_{A_j}^\dagger U_{B_k}^\dagger &= \omega^{-\delta_{jk}}, \\ U_{A_j} U_{A_k} U_{A_j}^\dagger U_{A_k}^\dagger &= 1, \\ U_{B_j} U_{B_k} U_{B_j}^\dagger U_{B_k}^\dagger &= 1, \quad j, k = 1, 2, \dots, n. \end{aligned} \tag{A.4}$$

According to the multipartite analogy of the Weyl's theorem [31, 32], the representation must have degree p^n and the image must be (projectively) unitarily equivalent to the multipartite HW group in dimension p^n . \square

Appendix B. Proof of Lemma 6

Proof. Suppose on the contrary that the SIC $\{\Pi_j\}$ is quasi-triply covariant. Then it is necessarily doubly covariant, that is, super-symmetric, given that the symmetry group of the SIC is a normal subgroup of the extended symmetry group of index at most 2. In addition, the normalized triple products \tilde{T}_{jkl} for distinct j, k, l can take on at most two different values, which are conjugate phase factors, say t and t^* . If $t = \pm 1$, then the same proof of Lemma 5 applies. Similar reasoning also shows that t cannot equal $\pm i$ when $d \geq 3$.

Now suppose that $t^4 \neq 1$. Since the SIC $\{\Pi_j\}$ is super-symmetric, the multiset $\{\tilde{T}_{mjk}\}_{m=1}^{d^2}$ is invariant under complex conjugation and is independent of j, k as long as j, k are distinct. It follows that the multiset contains two copies of 1 and $(d^2 - 2)/2$ copies of t and t^* . This observation implies the lemma immediately when d is odd. In general, choose a triple j, k, l such that $T_{jkl} = t$. According to Eq. (12) and the assumption $t^4 \neq 1$, if m is distinct from j, k, l , then two of the three numbers $\tilde{T}_{mjk}, \tilde{T}_{mkl}, \tilde{T}_{mlj}$ are equal to t and one equal to t^* . It follows that the three multisets $\{\tilde{T}_{mjk}\}_{m=1}^{d^2}$, $\{\tilde{T}_{mkl}\}_{m=1}^{d^2}$, and $\{\tilde{T}_{mlj}\}_{m=1}^{d^2}$ contain at least $2(d^2 - 3)$ copies of t in total. Therefore, $2(d^2 - 3) \leq 3(d^2 - 2)/2$, that is, $d^2 \leq 6$, which can never hold when $d \geq 3$. \square

Appendix C. Permutation groups

For the convenience of the reader, in this appendix we introduce several basic concepts and results about permutation groups that are relevant to the study in the main text; see Refs. [39, 40, 53] for more details.

Given a finite set $\Omega = \{\alpha, \beta, \dots\}$ with n elements, the group composed of all permutations on Ω is called the symmetric group on Ω and denoted by S_Ω . The group S_Ω is isomorphic to the symmetric group of the set $\{1, 2, \dots, n\}$, which is usually denoted by S_n . A group action of G on Ω is a map from the Cartesian product $G \times \Omega$ to Ω that satisfies $1\alpha = \alpha$ and $g(h\alpha) = (gh)\alpha$, where 1 denotes the identity of G (and also the trivial group with only one element) and $g\alpha$ denotes the image of the pair (g, α) under the map. An *orbit* is the set of images of a point $\alpha \in \Omega$ (elements of Ω are usually referred to as points) under the action of G , that is, $\{g\alpha : g \in G\}$. All orbits of the action form a partition of Ω . The *stabilizer* G_α of a point α is the group composed of all elements g that leave α invariant, that is, $g\alpha = \alpha$. The *kernel* of the action is the group composed of all elements g that act trivially on Ω , that is, $g\alpha = \alpha$ for all $\alpha \in \Omega$. By definition, the kernel is the intersection $\bigcap_{\alpha \in \Omega} G_\alpha$ of all point stabilizers. Alternatively, a group action of G on Ω is a homomorphism from G to S_Ω , and the kernel of the action coincides with the kernel of the homomorphism. The action is *faithful* if the kernel is trivial. A *permutation group* on Ω is a group G that acts faithfully on Ω , which can be identified as a subgroup of S_Ω . The *degree* of the permutation group is the cardinality of Ω .

A permutation group G on Ω is *transitive* if every element in Ω can be mapped to every other one under the action of G . In that case, all point stabilizers are conjugate to each other, and the order of G is equal to the product of the order of each point stabilizer and the cardinality of Ω , that is, $|G| = |G_\alpha||\Omega|$. A transitive group is *regular* if each point stabilizer is trivial, in which case $|G| = |\Omega|$. The group G is *k-transitive* if every ordered k -tuple of distinct elements of Ω can be mapped to every other such k -tuple. When $k > 1$, a group is *k-transitive* if and only if it is transitive and each point stabilizer is $(k - 1)$ -transitive on the remaining points. A *k-transitive* group is *sharply k-transitive* if each k -point stabilizer is trivial. The group G is *k-homogeneous* if every unordered k -tuple of distinct elements can be mapped to every other such k -tuple. By definition, a permutation group of degree n is *k-homogeneous* if and only if it is $(n - k)$ -homogeneous. In addition, every *k-transitive* permutation group is *k-homogeneous*.

A *block* Δ (also called a set of imprimitivity) of the action of G on Ω is a nonempty subset of Ω such that $g\Delta := \{g\alpha : \alpha \in \Delta\}$ for any $g \in G$ is either

identical with Δ or disjoint from Δ . The block is nontrivial if it is a proper subset of Ω that contains more than one elements. A transitive permutation group is *imprimitive* if there exists a nontrivial block and *primitive* otherwise. Alternatively, the group is primitive if no nontrivial partition of Ω is left invariant, where a partition is nontrivial if it has at least two components each of which has at least two points. Primitive permutation groups play a crucial role in the study of permutation groups. Their basic properties are listed below for easy reference.

1. A permutation group G is primitive if and only if each point stabilizer is a maximal subgroup of G .
2. Every normal subgroup $N \neq 1$ of a primitive permutation group G on Ω acts transitively on Ω .
3. Every 2-transitive permutation group is primitive.

Remark 9. A *maximal subgroup* M of a group G is a proper subgroup that is not contained in any other proper subgroup.

To better understand the properties of primitive and 2-transitive permutation groups, we need to introduce several new concepts. A *minimal normal subgroup* N of a group G is a normal subgroup other than the identity that contains no other nontrivial normal subgroup of G . Any minimal normal subgroup is a direct product of isomorphic simple groups. Any two distinct minimal normal subgroups of a given group have a trivial intersection and commute with each other. The *socle* of a group G is the product of all minimal normal subgroups of G and is denoted by $\text{soc}(G)$; it is a characteristic subgroup of G . Recall that a characteristic subgroup of G is a subgroup that is invariant under all automorphisms of G . The structure of minimal normal subgroups of a primitive permutation group is characterized by Theorem 4.3B in Ref. [39], as reproduced here.

Theorem 5. *If G is a finite primitive permutation group on Ω , and N a minimal normal subgroup of G , then exactly one of the following holds:*

1. N is a regular elementary abelian group, and $\text{soc}(G) = N = C_G(N)$.
2. N is a regular nonabelian group, $C_G(N)$ is a minimal normal subgroup of G which is permutation isomorphic to N , and $\text{soc}(G) = N \times C_G(N)$.
3. N is nonabelian, $C_G(N) = 1$, and $\text{soc}(G) = N$.

Remark 10. An elementary abelian group is the direct product of cyclic groups of the same prime order. Here $C_G(N)$ denotes the centralizer of N in G . Two permutation groups on Ω are *permutation isomorphic* if they are conjugate to each other under S_Ω . This theorem implies that a primitive

permutation group has at most two minimal normal subgroups. It has only one minimal normal subgroup if the socle is abelian. Note that the socle of a primitive permutation group is abelian if and only if one minimal normal subgroup is abelian.

Appendix D. Proof of Lemma 12

Proof. Note that any subgroup of index 2 is normal, that any 2-transitive permutation group is primitive, and that any nontrivial normal subgroup of a primitive permutation group is transitive [39, 40, 53]. It follows that H is a transitive normal subgroup of G . In addition, the point stabilizer H_α of any point $\alpha \in \Omega$ has either one orbit or two orbits of equal length on the remaining points of Ω . In the former case, H is 2-transitive and is thus primitive; in the latter case, it is also straightforward to show that H is primitive. According to Theorem 5, H has either one or two minimal normal subgroups, and in the latter case the two minimal normal subgroups are nonabelian regular and are centralizers of each other².

Let N be the unique minimal normal subgroup of G . Then N is contained in H and contains one of the minimal normal subgroups of H , say M . According to Burnside's theorem (Theorem 3 in the main text) on 2-transitive permutation groups [39, 40], N is either elementary abelian regular or nonabelian simple, and the centralizer $C_G(N)$ is either identical with N or trivial accordingly. Therefore, M must be identical with N since it is either a transitive subgroup of the regular group N or a normal subgroup of the simple group N . Consequently, the centralizer $C_H(M)$ is either identical with M or trivial. It follows from Theorem 5 that H has a unique minimal normal subgroup, which coincides with the unique minimal normal subgroup of G . \square

Appendix E. Proof of Lemma 13

All 2-transitive permutation groups have been classified by Huppert [47] and Hering [48, 49] (see also Refs. [39, 40]), with the aid of the classification of finite simple groups (CFSG) [22, 23]. Almost simple 2-transitive permutation groups are listed in Table 7.4 in Ref. [40]. According to this table, if the minimal normal subgroup (socle) N of the group is not the alternating group A_n for $n \geq 5$, then the degree n can only take on the following values:

²The author is grateful to Dragomir Ž Đoković for simplifying the proof of Lemma 12.

1. $(q^k - 1)/(q - 1)$ with $k \geq 2$ and $(k, q) \neq (2, 2), (2, 3)$;
2. $2^{2k-1} + 2^{k-1}$ with $k \geq 3$;
3. $2^{2k-1} - 2^{k-1}$ with $k \geq 3$;
4. $q^3 + 1$ with $q \geq 3$;
5. $q^2 + 1$ with $q = 2^{2k+1} > 2$;
6. 11, 12, 15, 22, 23, 24, 28, 176, 276;

where q is a prime power and k a positive integer.

In case 1, N is isomorphic to $\text{PSL}(k, q)$. According to Lemma 18 below, the degree n is a perfect square if and only if $(k, q) = (2, 8), (4, 7)$, or $(5, 3)$, in which case n is equal to $3^2, 20^2$, or 11^2 accordingly.

In case 2, N is isomorphic to $\text{Sp}(2k, 2)$. According to Lemma 17 below, the degree n is a perfect square if and only if $k = 3$, in which case n is equal to 6^2 .

In case 3, the degree can never be a perfect square according to Lemma 17. In cases 4 and 5, the degree can never be a perfect square according to Lemma 15 below. In case 6, the degree can never be a perfect square by direct inspection. This observation completes the proof of Lemma 13.

Lemma 15. *Suppose q is a prime power and m a positive integer. Then $q + 1$ is a perfect square if and only if $q = 3$ or $q = 8$; $q^m + 1$ is a perfect square if and only if $(m, q) = (1, 3), (1, 8)$, or $(3, 2)$.*

Proof. Obviously $q + 1$ is a perfect square when $q = 3$ or $q = 8$. Suppose $q = p^j$ and $q + 1 = b^2$, where p is a prime, and j, b are positive integers. Then $p^j = (b - 1)(b + 1)$. If $q > 3$ then $b > 2$, so p divides both $b - 1$ and $b + 1$ and thus equals 2. Consequently, both $b - 1$ and $b + 1$ must be powers of 2. It follows that $b = 3$ and $q = 8$. The second part of the lemma is an immediate consequence of the first part given that q^m is also a prime power. \square

Lemma 16. *Suppose q is a power of the prime p and $j \geq k$ are nonnegative integers. Then $q^j + q^k$ is a perfect square if and only if one of the following conditions is satisfied*

1. $j = k$ is odd and q is an odd power of 2.
2. q^k is a perfect square and $(j - k, q) = (1, 3), (1, 8)$, or $(3, 2)$.

Proof. If $j = k$, then $q^j + q^k = 2q^j$, which is a perfect square if and only if j is odd and q is an odd power of 2. If $j > k$, then $q^j + q^k = q^k(q^m + 1)$ with $m = j - k$. If q^k is not a perfect square, then $q^j + q^k$ is a perfect square if and only if $p(q^m + 1)$ is a perfect square, which is impossible. Otherwise, $q^m + 1$ is a perfect square, so $(m, q) = (1, 3), (1, 8)$, or $(3, 2)$ according to Lemma 15. \square

Lemma 17. *Suppose $j > k$ are nonnegative integers. Then $2^j + 2^k$ is a perfect square if and only if k is even and $j = k + 3$; $2^j - 2^k$ is a perfect square if and only if k is even and $j = k + 1$.*

Proof. The first statement follows from Lemma 16. If k is odd, then $2^j - 2^k$ is a perfect square if and only if $2(2^m - 1)$ with $m = j - k$ is a perfect square, which is impossible. Otherwise, $2^j - 2^k$ is a perfect square if and only if $(2^m - 1)$ is a perfect square, say $2^m - 1 = b^2$ with b a positive integer. This is possible if and only if $m = 1$ given that $b^2 + 1$ is not divisible by 4. \square

Lemma 18. *Suppose q is a prime power and $k \geq 2$ a positive integer. Then $(q^k - 1)/(q - 1)$ is a perfect square if and only if the pair (k, q) takes on one of the four possible values $(2, 3)$, $(5, 3)$, $(4, 7)$, and $(2, 8)$.*

Proof. The equation

$$\frac{q^k - 1}{q - 1} = d^2 \tag{E.1}$$

with d a positive integer is a special instance of the Nagell-Ljunggren equation. If $k \geq 3$, then the only integer solutions are $(k, q, d) = (5, 3, 11)$ and $(k, q, d) = (4, 7, 20)$ [57–59]³.

If $k = 2$, then $(q^k - 1)/(q - 1) = q + 1$ is a perfect square if and only if $q = 3$ or $q = 8$ according to Lemma 15. \square

References

- [1] G. Zauner, Quantum designs: Foundations of a noncommutative design theory, *Int. J. Quant. Inf.* 9 (2011) 445–507.
- [2] J. M. Renes, R. Blume-Kohout, A. J. Scott, C. M. Caves, Symmetric informationally complete quantum measurements, *J. Math. Phys.* 45 (2004) 2171, supplementary information including the fiducial kets available at <http://www.cquic.org/papers/reports/>.
- [3] A. J. Scott, M. Grassl, Symmetric informationally complete positive-operator-valued measures: A new computer study, *J. Math. Phys.* 51 (2010) 042203, supplementary information including the fiducial kets available at <http://arxiv.org/abs/0910.5784>.

³The author is grateful to Gergely Harcos for helping proving Lemma 18 by introducing the concept of Nagell-Ljunggren equation and Ref. [58] and to Daniel El-Baz for recommending Ref. [57] in response to a question posed by the author on MathOverflow.

- [4] H. Zhu, Quantum state estimation and symmetric informationally complete POMs, Ph.D. thesis, National University of Singapore, available at <http://scholarbank.nus.edu.sg/bitstream/handle/10635/35247/ZhuHJthesis.pdf> (2012).
- [5] D. M. Appleby, C. A. Fuchs, H. Zhu, Group theoretic, Lie algebraic and Jordan algebraic formulations of the SIC existence problem, *Quantum Inf. Comput.* 15 (1-2) (2015) 61–94.
- [6] C. A. Fuchs, R. Schack, Quantum-Bayesian coherence, *Rev. Mod. Phys.* 85 (2013) 1693–1715.
- [7] I. Bengtsson, K. Życzkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement*, Cambridge University Press, Cambridge, UK, 2006.
- [8] D. M. Appleby, Å. Ericsson, C. A. Fuchs, Properties of QBist state spaces, *Found. Phys.* 41 (2011) 564.
- [9] A. J. Scott, Tight informationally complete quantum measurements, *J. Phys. A: Math. Gen.* 39 (2006) 13507.
- [10] H. Zhu, B.-G. Englert, Quantum state tomography with fully symmetric measurements and product measurements, *Phys. Rev. A* 84 (2011) 022327.
- [11] H. Zhu, Quantum state estimation with informationally overcomplete measurements, *Phys. Rev. A* 90 (2014) 012115.
- [12] H. Zhu, Tomographic and Lie algebraic significance of generalized symmetric informationally complete measurements, *Phys. Rev. A* 90 (2014) 032309.
- [13] D. Petz, L. Ruppert, Efficient quantum tomography needs complementary and symmetric measurements, *Rep. Math. Phys.* 69 (2) (2012) 161–177.
- [14] C. A. Fuchs, M. Sasaki, Squeezing quantum information through a classical channel: Measuring the “quantumness” of a set of quantum states, *Quant. Inf. Comput.* 3 (5) (2003) 377–404.
- [15] J. M. Renes, Frames, designs, and spherical codes in quantum information theory, Ph.D. thesis, The University of New Mexico (2004).

- [16] J. M. Renes, Equiangular spherical codes in quantum cryptography, *Quantum Inf. Comput.* 5 (2005) 81.
- [17] B.-G. Englert, D. Kaszlikowski, H. K. Ng, W. K. Chua, J. Řeháček, J. Anders, Efficient and robust quantum key distribution with minimal state tomography, available at <http://arxiv.org/abs/quant-ph/0412075> (2004).
- [18] T. Durt, C. Kurtsiefer, A. Lamas-Linares, A. Ling, Wigner tomography of two-qubit states and quantum cryptography, *Phys. Rev. A* 78 (2008) 042338.
- [19] S. D. Howard, A. R. Calderbank, W. Moran, The finite Heisenberg-Weyl groups in radar and communications, *EURASIP J. Appl. Signal Processing* 2006 (2006) 85685.
- [20] D. M. Appleby, C. A. Fuchs, H. Zhu, unpublished (2014).
- [21] H. Zhu, Permutation symmetry determines the discrete Wigner function (2015). [arXiv:1504.03773](https://arxiv.org/abs/1504.03773).
- [22] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *An ATLAS of Finite Groups*, Oxford University Press, Oxford, 1985.
- [23] R. A. Wilson, *The Finite Simple Groups*, Vol. 251 of Graduate Texts in Mathematics, Springer, London, 2009.
- [24] D. M. Appleby, Symmetric informationally complete-positive operator valued measures and the extended Clifford group, *J. Math. Phys.* 46 (2005) 052107.
- [25] H. Zhu, SIC POVMs and Clifford groups in prime dimensions, *J. Phys. A: Math. Theor.* 43 (2010) 305305.
- [26] L. Hughston, $d = 3$ SIC-POVMs and elliptic curves, Perimeter Institute, seminar talk, available online at <http://pirsa.org/07100040/> (2007).
- [27] I. Bengtsson, From SICs and MUBs to Eddington, *J. Phys. Conf. Ser.* 254 (2010) 012007.
- [28] G. N. M. Tabia, D. M. Appleby, Exploring the geometry of qutrit state space using symmetric informationally complete probabilities, *Phys. Rev. A* 88 (2013) 012131.

- [29] H. B. Dang, K. Blanchfield, I. Bengtsson, D. M. Appleby, Linear dependencies in Weyl–Heisenberg orbits, *Quantum Inf. Process.* 12 (11) (2013) 3449–3475.
- [30] S. G. Hoggar, 64 lines from a quaternionic polytope, *Geom. Dedicata* 69 (1998) 287.
- [31] B. Bolt, T. G. Room, G. E. Wall, On the Clifford collineation, transform and similarity groups. I., *J. Austral. Math. Soc.* 2 (1961) 60–79.
- [32] B. Bolt, T. G. Room, G. E. Wall, On the Clifford collineation, transform and similarity groups. II., *J. Austral. Math. Soc.* 2 (1961) 80–96.
- [33] H. Zhu, Mutually unbiased bases as minimal Clifford covariant 2-designs, *Phys. Rev. A* 91 (2015) 060301.
- [34] W. K. Wootters, A Wigner-function formulation of finite-state quantum-mechanics, *Ann. Phys.* 176 (1) (1987) 1–21.
- [35] H. Zhu, in preparation (2015).
- [36] L. Hughston, S. Salamon, Surveying points in the complex projective plane (2014). [arXiv:1410.5862](https://arxiv.org/abs/1410.5862).
- [37] H. Zhu, Sharply covariant mutually unbiased bases (2015). [arXiv:1503.00003](https://arxiv.org/abs/1503.00003).
- [38] H. Zhu, Nonexistence of sharply covariant mutually unbiased bases in odd prime dimensions, to appear in *Phys. Rev. A.* (2015). [arXiv:1506.05737](https://arxiv.org/abs/1506.05737).
- [39] J. D. Dixon, B. Mortimer, *Permutation Groups*, Vol. 163 of Graduate Texts in Mathematics, Springer, New York, 1996.
- [40] P. J. Cameron, *Permutation Groups*, Vol. 45 of London Mathematical Society Student Texts, Cambridge University Press, Cambridge, UK, 1999.
- [41] D. Gottesman, Stabilizer codes and quantum error correction, Ph.D. thesis, California Institute of Technology, available at <http://arxiv.org/abs/quant-ph/9705052> (1997).
- [42] H. Weyl, *The Theory of Groups and Quantum Mechanics*, Methuen & co. ltd., London, 1931, translated from the second (revised) German edition by H. P. Robertson.

- [43] D. E. Taylor, The geometry of the classical groups, Vol. 9 of Sigma Series in Pure Mathematics, Heldermann Verlag, 1992.
- [44] A. O. Morris, Projective representations of Abelian groups, J. London Math. Soc. s2-7 (2) (1973) 235–238.
- [45] H. Zhu, Y. S. Teo, B.-G. Englert, Minimal tomography with entanglement witnesses, Phys. Rev. A 81 (2010) 052339.
- [46] H. Zhu, Y. S. Teo, B.-G. Englert, Two-qubit symmetric informationally complete positive-operator-valued measures, Phys. Rev. A 82 (2010) 042308.
- [47] B. Huppert, Zweifach transitive, auflösbare Permutationsgruppen, Mathematische Zeitschrift 68 (1) (1957) 126–150.
- [48] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, Geom. Dedicata 2 (4) (1974) 425–460.
- [49] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II, J. Algebra 93 (1) (1985) 151–164.
- [50] W. M. Kantor, k -homogeneous groups, Mathematische Zeitschrift 124 (4) (1972) 261–265.
- [51] D. M. Appleby, S. T. Flammia, C. A. Fuchs, The Lie algebraic significance of symmetric informationally complete measurements, J. Math. Phys. 52 (2011) 022202.
- [52] R. B. Ash, Basic Abstract Algebra: For Graduate Students and Advanced Undergraduates, Dover, New York, 2007.
- [53] H. Kurzweil, B. Stellmacher, The Theory of Finite Groups: An Introduction, Springer, New York, 2004.
- [54] E. Weiss, Algebraic Number Theory, McGraw-Hill Book Company, Inc., New York, 1963.
- [55] P. H. Tiep, A. E. Zalesskii, Minimal characters of the finite classical groups, Commun. Algebra 24 (6) (1996) 2093–2167.

- [56] C. Bessenrodt, H. N. Nguyen, J. B. Olsson, H. P. Tong-Viet, Complex group algebras of the double covers of the symmetric and alternating groups, *Algebra & Number Theory* 9 (3) (2015) 601–628.
- [57] P. Ribenboim, *Catalan’s Conjecture: Are 8 and 9 the Only Consecutive Powers?*, Academic Press, 1994.
- [58] W. Ljunggren, Noen setninger om ubestemte likninger av formen $(x^n - 1)/(x - 1) = y^q$, *Norsk. Mat. Tidsskr.* 25 (1943) 17–20.
- [59] Y. Bugeaud, P. Mihăilescu, On the Nagell-Ljunggren equation $(x^n - 1)/(x - 1) = y^q$, *Math. Scand.* 101 (2007) 177–183.